

## AFMSS Assessment Findings

There were 20 findings for the AFMSS; the following are the findings in the initial assessment:

1. No application user-ID (I&A compliance) \*\*
2. Lack of strong password composition (I&A compliance) \*\*
3. Passwords are not changed at regular intervals for regular users as well as administrators (I&A compliance)\*\*
4. Passwords are not monitored for ageing (I&A Compliance) \*\*
5. Old User-ids are still on the AFMSS systems (Password Management) \*\*
6. No user termination procedures in effect (Access control) \*\*
7. No inactivity logoff (Access control) \*\*
8. Stored system passwords are not encrypted (Access control) \*\*
9. No audit trails in AFMSS (Audit) \*\*
10. No audit trails in Informix (Audit) \*\*
11. AFMSS Data is modifiable outside the application (Access/audit) \*\*
12. No Security Training (Security Training and Awareness) \*
13. No refresher security training (Security Training and Awareness) \*
14. No Rules of Behavior (Security Plan) \*
15. Configuration Management of application in the hands of the system user. (Configuration Management) \*\*
16. No Certification Statement for AFMSS (Security Management) \*\*
17. No Accreditation Statement for AFMSS (Security Management) \*\*
18. No Security Test Plan for AFMSS (Software Security) \*
19. No Banner Pages before access to application (Software Security) \*
20. Contingency Plan has not been tested (Security Management) \*\*

\* Legislation Requirement

\*\* Regulation Requirement